4H

УДК 004.415.24; 004.932.2

Л.Л. Нікітенко, О.Ю. Нікітіна
Інститут кібернетики імені В.М. Глушкова НАН України, м. Київ
zvk140@ukr.net, nikitinao@ukr.net

Вкраплення додаткової інформації в частотну область цифрового сигналу

Запропоновано метод вкраплення цифрових водяних знаків в частотно-часове представлення сигналу. Поворот обраних фазових складових сигналу на певний кут здійснюється за рахунок незначної зміни певних відліків початкового сигналу. Проведені теоретичні дослідження з метою зменшення кількості обчислень. Запропоновано послідовність дій для вибору оптимального значення вектору змін.

Потреба створення універсальних стеганографічних методів захисту цифрової інформації є однією з найбільш актуальних наукових задач сьогодення. Вкраплення цифрових водяних знаків (ЦВЗ) у цифрові сигнали (ЦС) є одним з методів захисту цифрової інформації. Такий захист вважається найбільш перспективним, тому його розвиток в першу чергу потребує теоретичних досліджень для створення надійних методів вкраплення [1]. Оскільки факт наявності ЦВЗ не завжди приховується, головною вимогою до побудови стеганосистеми з ЦВЗ є стійкість до типових активних атак на стеганоконтейнер, серед яких згладжування, стиск, зміна формату та ін. [2]. При такій постановці задачі під стійкістю ЦВЗ прийнято розуміти складність видалення або псування ЦВЗ без порушення функціональності контейнера. Вкраплення ЦВЗ може здійснюватися як у просторовій області, так і у частотній. Частотне представлення сигналу, як правило, отримують за допомогою дискретного перетворення Фур'є (ДПФ), дискретного косинус-перетворення або вейвлет-перетворення.

При використанні ДПФ зазвичай інформацію вкраплюють в амплітуди сигналу [3]. За рахунок певної надмірності інформації в амплітудах таке втручання не впливає на функціональність сигналу. З точки зору забезпечення стійкості до активних атак краще вкраплювати ЦВЗ у фази сигналу, оскільки більшість методів обробки сигналу використовує амплітуди при обробці сигналу. Втручання у фази призводить до значного спотворення сигналу при оберненому перетворенні, оскільки у загальному випадку при зміні фази компонентів повернутися в дійсну просторову область не завжди вдається.

У запропонованому методі ЦВЗ вкраплюється в частотно-часове представлення сигналу поворотом обраних фазових складових сигналу на певний кут за рахунок незначної зміни певних відліків початкового сигналу. Функціональність сигналу при оберненому ДПФ при цьому не порушується. Для вилучення ЦВЗ до стеганоключа додаються номери компонентів, фази яких при вкрапленні змінювалися до потрібного значення.

Найпростіший і водночас найдовший шлях вирішення поставленого завдання – це послідовна зміна всіх відліків вхідного сигналу доти, доки фаза потрібного компонента не досягне шуканої величини. В даній роботі ми намагаємося зменшити кількість обчислень, теоретично досліджуючи, як зміни в просторовій області відображаються в області Фур'є.

Нехай маємо дійсний дискретний сигнал g довжиною N відліків (контейнер)

$$g = [g_0, g_1, ..., g_{N-1}]. \qquad (1)$$

Дискретне перетворення Фур'є [4] переводить його в комплексну область $G = G_0, G_2, ..., G_{N-1}$, де

$$G_\nu = \frac{1}{N}\sum_{n=0}^{N-1} g_n \exp\left(-\frac{2\pi i n\nu}{N}\right), 0 \le \nu < N-1 .$$

Зміна відліків сигналу g_n на величини Δ_n, $n = \overline{0, N-1}$, призводить до зміни значень компонентів G_ν відповідно до виразу $G_\nu^{'} = G_\nu + R_\nu$ [5], де

$$R_\nu = \frac{1}{N}\sum_{n=0}^{N-1} \Delta_n \exp\left(-\frac{2\pi i n\nu}{N}\right). \quad (2)$$

Скориставшись формулою Ейлера $\exp(i\varphi) = \cos(\varphi) + i\sin(\varphi)$, довільне комплексне число $\exp(i\varphi)$ представимо у вигляді одиничного вектора $\vec{e}_\varphi = \vec{e}_1\cos(\varphi) + \vec{e}_2\sin(\varphi)$ у двовимірному ортогональному базисі $(\vec{e}_1, \vec{e}_2)$, де $\vec{e}_1$ та $\vec{e}_2$ – вектори одиничної довжини (рис. 1).

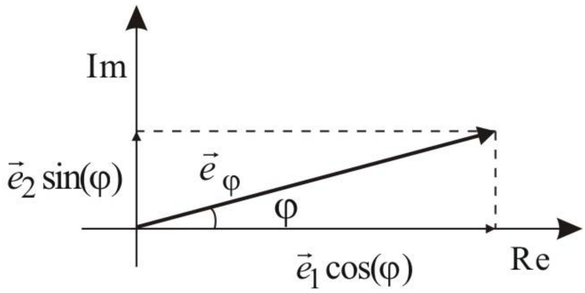


Рисунок 1 – Представлення величини $\exp(i\varphi)$ в ортогональному базисі $(\vec{e}_1, \vec{e}_2)$

Введемо позначення: a_ν – амплітуда компонента G_ν (довжина вектора $\vec{G}_\nu$), φ_ν – фаза G_ν (кут, який утворює вектор $\vec{G}_\nu$ з дійсною віссю); $a_\nu^{'}$ та $(\varphi_\nu + \Delta\varphi_\nu)$ – відповідно амплітуда та фаза $\vec{G}_\nu^{'}$; r_ν та θ_ν – відповідно амплітуда та фаза $\vec{R}_\nu$. З урахуванням позначень справедливі вирази

$$\vec{G}_\nu = a_\nu(\vec{e}_1\cos\varphi_\nu + \vec{e}_2\sin\varphi_\nu),$$
$$\vec{G}_\nu^{'} = a_\nu^{'}\left(\vec{e}_1\cos(\varphi_\nu + \Delta_{\varphi_\nu}) + \vec{e}_2\sin(\varphi_\nu + \Delta_{\varphi_\nu})\right),$$
$$\vec{R} = r_\nu(\vec{e}_1\cos\theta_\nu + \vec{e}_2\sin\theta_\nu).$$

Задача зводиться до пошуку вектора $\vec{R}_\nu$.

У векторному просторі значення доданка R_ν можна інтерпретувати як різницю векторів $\vec{G}_\nu^{'}$ та $\vec{G}_\nu$, кут між якими складає $\Delta\varphi_\nu$ (рис. 2).

З трикутника, утвореного векторами $\vec{G}_\nu$, $\vec{G}_\nu^{'}$ та $\vec{R}_\nu$, за теоремою косинусів

$$(r_\nu)^2 = (a_\nu)^2 + (a_\nu^{'})^2 - 2a_\nu a_\nu^{'}\cos(\Delta\varphi_\nu). \quad (3)$$

З теореми синусів $\dfrac{r_\nu}{\sin\Delta\phi_\nu} = \dfrac{a_\nu}{\sin\gamma_\nu}$ отримуємо $\sin\gamma_\nu = \dfrac{a_\nu}{r_\nu}\sin(\Delta\varphi_\nu)$.

З рис. 2 знаходимо

$$\theta_\nu = \varphi_\nu + \Delta\varphi_\nu + \gamma_\nu . \qquad (4)$$

З (3) знаходиться амплітуда r_ν, з (4) – фаза θ_ν компонента R_ν:

$$\theta_\nu = \varphi_\nu + \Delta\varphi_\nu + \arcsin\left(\frac{\alpha_\nu \sin(\Delta\varphi_\nu)}{r_\nu}\right), \qquad (5)$$

з обмеженням

$$-\frac{\pi}{2} < \frac{\alpha_\nu \sin(\Delta\phi_\nu)}{r_\nu} < \frac{\pi}{2} . \qquad (6)$$

З урахуванням співвідношень (3), (5)

$$R_\nu = r_\nu \exp\left(-i\left(\varphi_\nu + \Delta\varphi_\nu + \arcsin\left(\frac{\alpha_\nu \sin(\Delta\varphi_\nu)}{r_\nu}\right)\right)\right). \qquad (7)$$

Прирівняємо праві частини (2) та (7):

$$\frac{1}{N}\sum_{n=0}^{N-1}\Delta_n \exp\left(-\frac{2\pi i n}{N}\nu\right) = r_\nu \exp(-i(\varphi_\nu + \Delta\varphi_\nu + \gamma_\nu)). \qquad (8)$$

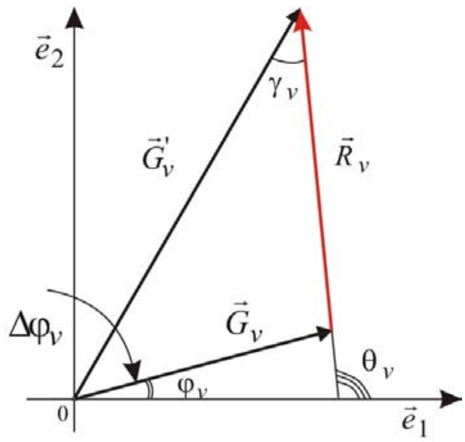


Рисунок 2 – Вектор різниці $\vec{R}_\nu = \vec{G}'_\nu - \vec{G}_\nu$

Рівняння (3) обмежує амплітуду r_ν. Для того щоб зміни початкових відліків сигналу не були помітні в області Фур'є, a'_ν та a_ν не повинні сильно відрізнятися. Позначимо $(a'_\nu - a_\nu) = \delta$, тоді з (3)

$$(r_\nu)^2 = (a_\nu)^2\left(2\left(1+\frac{\delta}{a_\nu}\right)(1-\cos(\Delta\varphi_\nu)) + \left(\frac{\delta}{a_\nu}\right)^2\right). \qquad (9)$$

З (9) видно, що для заданих a_ν та $\Delta\varphi_\nu$ обмеження по δ приводить до обмеження по r_ν. Оскільки за умовою задачі G_ν відомі, відповідно відомі й φ_ν та відомі бажані φ'_ν, тому $\Delta\varphi_\nu$ теж відомі. За допомогою (5) знаходимо θ_ν при відомих r_ν.

Потрібно мінімізувати зміни амплітуд компонентів сигналу. Крім того, рівняння (9) обмежує зміну кута вектора $\vec{G}_\nu$. За умови, що довжина вектора $\vec{R}_\nu$ менша довжи-

ни вектора $\vec{G}_\nu$, можна оцінити найбільшу величину кута $\Delta\varphi_\nu$ (рис. 3). Якщо навколо кінця вектора $\vec{G}_\nu$ окреслити коло радіусом r_ν та з початку вектора $\vec{G}_\nu$ провести дотичну до цього кола, тоді кут між дотичною та самим вектором $\vec{G}_\nu$ буде максимально можливим кутом $\Delta\varphi_\nu$. Враховуючи, що $\sin\Delta\varphi_\nu = \frac{|\vec{R}_\nu|}{|\vec{G}_\nu|}$, отримуємо $\Delta\varphi_{\nu\max} = \arcsin\frac{|\vec{R}_\nu|}{|\vec{G}_\nu|}$.

Бажано, щоб $\gamma_\nu = \pi/2$. Тоді з (4) отримуємо $\theta_\nu = \varphi_\nu + \Delta\varphi_\nu + \pi/2$. На практиці ми не завжди можемо вносити зміни у відліки початкового сигналу так, щоб досягти такого значення γ_ν, але завжди треба пам'ятати, що саме такий кут є бажаним для зменшення змін відліків вхідного сигналу.

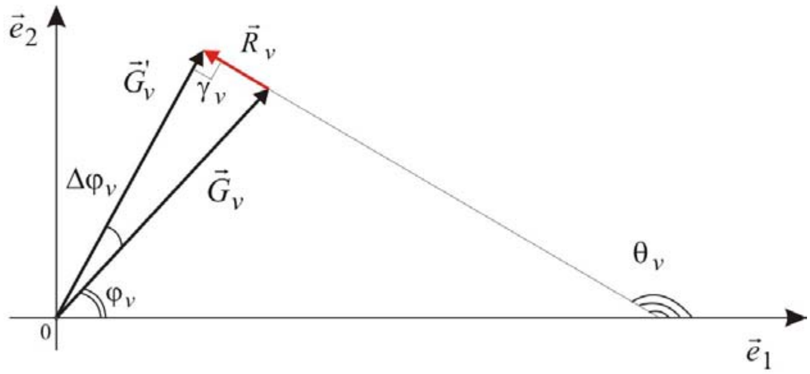


Рисунок 3 – Ілюстрація максимального значення кута $\Delta\varphi_\nu$

Послідовність дій для вибору оптимального значення $\vec{R}_\nu$ може бути наступною. При відомих ν та ψ визначити амплітуду та фазу ν-го компонента, вирахувати $\Delta\varphi_\nu$. Відповідно до рис. 3 від початку вектора $\vec{G}_\nu$ під кутом $\Delta\varphi_\nu$ провести промінь. З кінця вектора $\vec{G}_\nu$ опустити на цей промінь перпендикуляр. Напрямок даного перпендикуляра буде найбільш оптимальним напрямком вектора змін $\vec{R}_\nu$. У випадку, коли змінюється значення тільки одного відліку початкового сигналу, потрібно змінювати відлік з тим номером n, щоб $-\frac{2\pi in\nu}{N}$ було найбільш наближеним до оптимального напрямку $\vec{R}_\nu$.

В роботі [5] розглянуто випадок, коли амплітуди $\vec{G}_\nu$ та $\vec{G}'_\nu$ збігаються. Для нього була доведена наступна теорема.

Теорема. Для зміни фази $G_\nu = a\exp(i\varphi)$ на величину Δ_φ необхідно додати до G_ν величину $2a\sin\frac{\Delta\varphi}{2}\exp\left(i\left(\varphi+\frac{\Delta\varphi+\pi}{2}\right)\right)$:

$$a(\exp(i\varphi+\Delta_\varphi)) - a(\exp(i\varphi)) = 2a\sin\frac{\Delta\varphi}{2}\exp\left(i\left(\varphi+\frac{\Delta\varphi+\pi}{2}\right)\right). \quad (10)$$

Наслідок. З теореми випливає, що змінити фазу $g_\nu = a\exp(i\varphi)$ на величину Δ_φ можна, вносячи такі зміни в просторову область, щоб

$$2a\sin\frac{\Delta\varphi}{2}\exp\left(i\left(\varphi+\frac{\Delta\varphi+\pi}{2}\right)\right) = \frac{1}{N}\sum_{n=0}^{N}\Delta_n\exp\left(-\frac{2\pi in\nu}{N}\right). \quad (11)$$

Повернемося до загального випадку, коли змінюються і фаза і амплітуда ν-го компонента в області Фур'є. Розглянемо найпростіші випадки, коли змінюється один або два відліки вхідного сигналу. Нашим завданням є зміна φ_V на $\psi_v = \varphi_V + \Delta\varphi_V$ (далі $\psi_v = \psi$), з найменшими змінами відліків вхідного сигналу, тобто з найменшими значеннями Δ_n, $n = \overline{0, N-1}$.

Випадок 1. Зміни вносяться лише до одного відліку сигналу g в (1). Нехай $g_k^{'} = g_k + \Delta_k$ ($\Delta_k = \Delta$), тоді

$$R_v = \frac{\Delta}{N}\exp\left(-\frac{2\pi ikv}{N}\right).$$

Отже, $r_v = \frac{\Delta}{N}$, $\theta_v = -\frac{2\pi kv}{N}$, з обмеженням (6).

Потрібно визначити k та ν такі, щоб Δ було найменшим за абсолютною величиною. З (5) отримуємо

$$\arcsin\left(\frac{N\alpha_v \sin(\Delta\phi_v)}{\Delta}\right) = -\frac{2\pi kv}{N} - \psi, \text{ або } \frac{N\alpha_v \sin(\Delta\varphi_v)}{\Delta} = \sin\left(-\frac{2\pi kv}{N} - \psi\right),$$

або розглядаючи Δ як функцію від k

$$\Delta(k) = \frac{N\alpha_v \sin(\Delta\phi_v)}{\sin\left(-\frac{2\pi kv}{N} - \psi\right)}, \text{ при } \sin\left(-\frac{2\pi kv}{N} - \psi\right) \neq 0.$$

Шукана величина $\Delta_{\min}(k)$ може бути знайдена розв'язанням наступного рівняння

$$\Delta_{\min}(k) = \min_{k \in \overline{0, N-1}} \frac{N\alpha_v \sin(\Delta\phi_v)}{\sin\left(-\frac{2\pi kv}{N} - \psi\right)}, \text{ при } \sin\left(-\frac{2\pi kv}{N} - \psi\right) \neq 0. \tag{12}$$

З (12) видно, що потрібним є значення k, для якого $\left|\sin\left((-2\pi kv/N) - \psi\right)\right|$ досягає найбільшого значення за абсолютною величиною, тобто кут $\left((2\pi kv/N) + \psi\right)$ наближений до кута $\pm\pi/2$.

Розглянемо найпростіший приклад: нехай сигнал $g = [g_0, g_1, ..., g_{N-1}]$ є лінійним $g_i = a_0 + ib_0$, довжина блока $N = 8$. Як показали дослідження у роботі [5], найменше значення амплітуди в області Фур'є буде мати величина G_3, тому обираємо $\nu = 3$. На рис. 4 показані напрямки всіх складових вектора $\vec{R}_v$. Також на рис. 4 показано, як формується вектор $\vec{G}_v$, його довжина та напрямок. З цього ж рисунка видно, що для невеликих значень $\Delta\phi_v$ найкращим рішенням буде зміна п'ятого відліку (для від'ємного $\Delta\phi_v$) або шостого (для додатного $\Delta\phi_v$). Рівняння (11) дає той самий результат.

Випадок 2. Зміни вносяться до двох відліків сигналу g в (1). Нехай $g_k^{'} = g_k + \Delta$, $g_m^{'} = g_m + \Delta$, причому $k \neq m$. В області Фур'є ці зміни відіб'ються на значеннях всіх компонентів $R_v = \frac{\Delta}{N}\left(\exp\left(-\frac{2\pi ikv}{N}\right) + \exp\left(-\frac{2\pi imv}{N}\right)\right)$.

Скориставшись формулою Ейлера та тригонометричними рівняннями, можна виразити R_v одним комплексним числом

$$R_v = \frac{\Delta}{N}\left(\cos\frac{2\pi kv}{N} + \cos\frac{2\pi mv}{N} - i\left(\sin\frac{2\pi kv}{N} + \sin\frac{2\pi mv}{N}\right)\right) =$$

$$= \frac{2\Delta}{N}\left(\cos\frac{2\pi v}{N}(k+m)\cos\frac{2\pi v}{N}(k-m) - i\left(\sin\frac{2\pi v}{N}(k+m)\cos\frac{2\pi v}{N}(k-m)\right)\right) =$$

$$= \frac{2\Delta}{N}\cos\frac{2\pi v}{N}(k-m)\left(\cos\frac{2\pi v}{N}(k+m) - i\sin\frac{2\pi v}{N}(k+m)\right) =$$

$$= \frac{2\Delta}{N}\cos\frac{2\pi v}{N}(k-m)\exp\left(-i\frac{2\pi v}{N}(k+m)\right).$$

Отже, $R_v = r_v\ \exp(-i\theta_v)$, де $r_v = \frac{2\Delta}{N}\cos\frac{2\pi v}{N}(k-m)$, $\theta_v = \frac{2\pi v}{N}(k+m)$ з обмеженням (6).

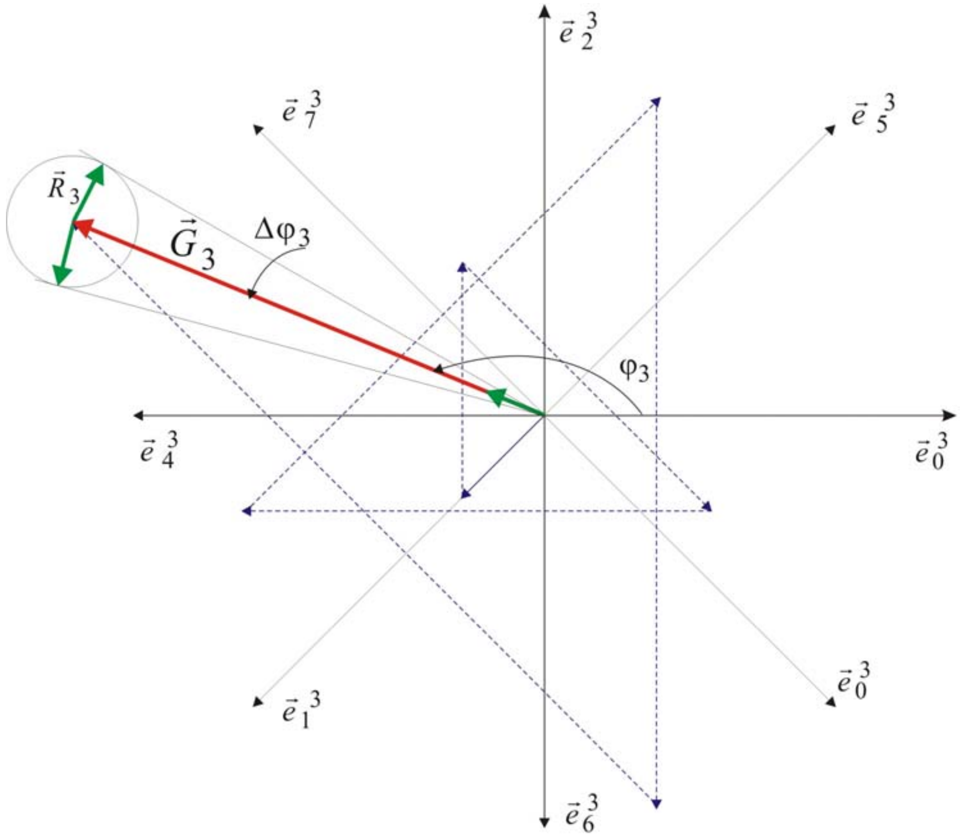


Рисунок 4 – Формування вектора $\vec{G}_3$ для випадку 2

Проводячи міркування, подібні до розглянутих вище для першого випадку, розглядаючи Δ як функцію від k, отримуємо при $\sin\left(\frac{2\pi v}{N}(k+m) - \varphi_v - \Delta\varphi_v\right) \neq 0$

$$\Delta_{\min}(k) = \min_{k \in \overline{0, N-1}} \frac{N\alpha_v \sin(\Delta\phi_v)}{\sin\left(\frac{2\pi v}{N}(k+m) - \phi_v - \Delta\phi_v\right)}. \qquad (13)$$

У випадку $g_k^{'} = g_k + \Delta$, $g_m^{'} = g_m - \Delta$, провівши перетворення, аналогічні попереднім, отримуємо

$$R_v = -\frac{2\Delta}{N} i \left(\sin\left(\frac{\pi v}{N}(k-m) \right) \exp\left(-\frac{\pi v i}{N}(k+m) \right) \right).$$

Проведені дослідження показали, що в загальному випадку, якщо всі відліки сигналу змінюються на величину Δ (або лишаються без змін), амплітуда R_v пропорційна $\frac{\Delta}{N}$, тобто $R_v = \frac{\Delta}{N} \sum_{n=0}^{N-1} \exp\left(-\frac{2\pi i n v}{N} \right)$. Це означає, що ми зможемо знайти оптимальне значення Δ з виразу (5), перебираючи тільки номери відліків, які зазнають змін під час вкраплення. За рахунок цього обчислювальна складність пошуку розв’язку поставленої задачі значно зменшується. В частинних випадках, розглянутих в роботі, вдалося отримати аналітичні рівняння для знаходження оптимального розв’язку поставленої задачі.

Зауважимо, що, з точки зору забезпечення функціональності сигналу, необхідно забезпечити відсутність сплеску амплітуд, особливо для низьких частот. Рівняння (9) дає зв’язок між величинами Δ та δ, що дозволяє контролювати сплески амплітуд.

Література

1. Грибунин В.Г. Цифровая стеганография / Грибунин В.Г., Оков И.Н., Туринцев И.В. – М. : Солон-Пресс, 2002. – 272 с.
2. Кошкина Н.В. К вопросу о защите интеллектуальной собственности на бумажных носителях / Н.В. Кошкина, О.Ю. Никитина // Материалы второй междунар. научной конф. по проблемам безопасности и противодействия терроризму. – М. : МЦНМО, 2007. – С. 304-307.
3. Никитина О.Ю. Оптимизация по точности методов цифровых водяных знаков, основанных на преобразовании Фурье-Меллина / О.Ю. Никитина // Искусственный интеллект. – 2007. – № 4. – С. 335-341.
4. Задирака В.К. Теория вычисления преобразования Фурье / Задирака В.К. – Киев : Наукова думка, 1983. – 215 с.
5. Никитенко Л.Л. Спектральные методы в компьютерной стеганографии. / Л.Л Никитенко, О.Ю. Никитина // Праці міжнародного симпозіуму «Питання оптимізації обчислень ПОО – XXXV», (Кацивелі, 24 – 29 вересня 2009 р.). – 2009. – Т. 2. – С. 150-155.

Л.Л. Никитенко, О.Ю. Никитина

Встраивание дополнительной информации в частотную область цифрового сигнала

Предложен метод встраивания цифровых водяных знаков в частотно-временное представление сигнала. Поворот выбранных фазовых составляющих на определенный угол осуществляется за счет незначительного изменения некоторых отсчетов входного сигнала. Проведены теоретические исследования с целью уменьшения объема вычислений. Предложена последовательность действий для выбора оптимального значения вектора изменений.

L. Nikitenko, O. Nikitina

The Side Information Hiding Into the Digital Signal Frequency Domain

Hiding method of the digital watermark into time-frequency signal notation was proposed. The selected phase term rotation on the preset angle was carrying out with insignificant changes of the some of the input signal components. The theoretical research es were made with the goal to reduce computing. The workflow was proposed to take change vector best value.

Стаття надійшла до редакції 06.07.2010.